What is claimed is:

1. A system for providing secure exchange of sensitive information with an implantable medical device, comprising:

a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session; and

an external source to securely obtain the crypto key over a secure connection from a secure key repository securely maintaining the crypto key, to encrypt the sensitive information using the crypto key and to store the sensitive information as encrypted data onto the implantable medical device.

2. A system according to Claim 1, further comprising:

a short range interface to logically define a secured area around the implantable medical device within which to securely obtain the crypto key; and

a long range interface to logically define a non-secured area extending beyond the secured area within which to exchange the encrypted data.

3. A system according to Claim 1, wherein the encrypted data is retrieved from the implantable medical device over a non-secure connection and the encrypted data is decrypted as the sensitive data using the crypto key.

4. A system according to Claim 3, wherein the crypto key is securely retrieved over a secure connection from the secure key repository prior to decrypting the encrypted data.

5. A system according to Claim 3, wherein the encrypted data is retrieved through long range telemetry.

6. A system according to Claim 5, wherein the long range telemetry comprises radio frequency telemetry.

7. A system according to Claim 1, wherein at least part of the sensitive information is securely stored as unencrypted data onto the implantable medical device over a secure connection.

8. A system according to Claim 7, wherein the unencrypted data is securely retrieved from the implantable medical device over a secure connection.

9. A system according to Claim 1, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

10. A system according to Claim 1, wherein the crypto key is maintained on the implantable medical device, and the crypto key is retrieved through short range telemetry.

11. A system according to Claim 10, wherein the short range telemetry comprises inductive telemetry.

12. A system according to Claim 1, wherein the external source comprises at least one of a programmer and a repeater.

13. A system according to Claim 1, wherein the crypto key comprises an encryption key in accordance with the Advanced Encryption Standard.

14. A method for providing secure exchange of sensitive information with an implantable medical device, comprising:

defining a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session;

securely obtaining the crypto key over a secure connection from a secure key repository securely maintaining the crypto key; and

encrypting the sensitive information using the crypto key and storing the sensitive information as encrypted data onto the implantable medical device.

15. A method according to Claim 14, further comprising:

logically defining a secured area around the implantable medical device within which to securely obtain the crypto key; and

logically defining a non-secured area extending beyond the secured area within which to exchange the encrypted data.

16. A method according to Claim 14, further comprising:

retrieving the encrypted data from the implantable medical device over a non-secure connection; and

decrypting the encrypted data as the sensitive data using the crypto key.

17. A method according to Claim 16, further comprising:

securely retrieving the crypto key over a secure connection from the secure key repository prior to decrypting the encrypted data.

18. A method according to Claim 16, further comprising:

retrieving the encrypted data through long range telemetry.

19. A method according to Claim 18, wherein the long range telemetry comprises radio frequency telemetry.

20. A method according to Claim 14, further comprising:

securely storing at least part of the sensitive information as unencrypted data onto the implantable medical device over a secure connection.

21. A method according to Claim 20, further comprising:

securely retrieving the unencrypted data from the implantable medical device over a secure connection.

22. A method according to Claim 14, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

23. A method according to Claim 14, further comprising:

maintaining the crypto key on the implantable medical device; and

retrieving the crypto key through short range telemetry.

24. A method according to Claim 23, wherein the short range telemetry comprises inductive telemetry.

25. A method according to Claim 14, wherein the external source comprises at least one of a programmer and a repeater.

26. A method according to Claim 14, wherein the crypto key comprises an encryption key in accordance with the Advanced Encryption Standard.

27. An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

means for defining a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session;

means for securely obtaining the crypto key over a secure connection from a secure key repository securely maintaining the crypto key; and

means for encrypting the sensitive information using the crypto key and means for storing the sensitive information as encrypted data onto the implantable medical device.

28. An implantable medical device for securely maintaining sensitive information, comprising:

an implantable medical device, comprising:

a memory to store sensitive information encrypted using a crypto key uniquely associated with an implantable medical device; and

a secure interface to provide access to the stored sensitive information exclusively over a secure connection.

29. An method for securely maintaining sensitive information on an implantable medical device, comprising:

storing sensitive information encrypted using a crypto key uniquely associated with an implantable medical device; and

providing access to the stored sensitive information exclusively over a secure connection.

30. An apparatus for securely maintaining sensitive information on an implantable medical device, comprising:

means for storing sensitive information encrypted using a crypto key uniquely associated with an implantable medical device; and

means for providing access to the stored sensitive information exclusively over a secure connection.